1/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:Derwent

010093179 **Image available**
WPI Acc No: 1994-360892/**199445**
XRPX Acc No: N94-282782
Key opening code system - calculates ellipse curve parameter from code sentence and common sentence obtained using calculation theorem
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 6282226	A	19941007	JP 9370436	A	19930329	199445	B

Priority Applications (No Type Date): JP 9370436 A 19930329
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 6282226	A		12	G09C-001/00	

Abstract (Basic): JP 6282226 A
The open key code system consists of an open file appts. (10) which chooses arbitrary prime numbers. The encryption keys corresp. to arbitrary prime numbers are formed by a key coding appts. (20). The decoding keys corresp. to the prime numbers are stored in a decoding key table of a decoder (40).
The open key of common sentence from the open file appts. is received and multiplied on an ellipse curve by an encryption appts. (30). The output of the encryption appts. is transmitted to the decoder as a code sentence. The ellipse curve parameter from the code sentence is calculated and the decoding key, corresponding to the parameter is selected from the decoding key table. Using a calculation theorem, the common sentence is obtained from the decoder.
ADVANTAGE - Prevents constraint of prime numbers of parameters. Provides safety.
Dwg.1/6
Title Terms: KEY; OPEN; CODE; SYSTEM; CALCULATE; ELLIPSE; CURVE; PARAMETER; CODE; SENTENCE; COMMON; SENTENCE; OBTAIN; CALCULATE; THEOREM
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00
International Patent Class (Additional): H04L-009/06; H04L-009/14
File Segment: EPI; EngPI

1/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

04610326 **Image available**
ELLIPTIC CURVE-BASED PUBLIC-KEY CIPHER SYSTEM

PUB. NO.: 06-282226 **JP 6282226** A]
PUBLISHED: October 07, 1994 (19941007)
INVENTOR(s): KUWAKADO SHUSUKE
KOYAMA KENJI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 05-070436 [JP 9370436]
FILED: March 29, 1993 (19930329)
INTL CLASS: [5] G09C-001/00; H04L-009/06; H04L-009/14
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 44.3 (COMMUNICATION -- Telegraphy)
JOURNAL: Section: , Section No. FFFFFF, Vol. 94, No. 10, Pg. FFFFFF, FF, FFFF (FFFFFFFF)

ABSTRACT

PURPOSE: To provide an elliptic curve-based public-key enciphering system having much enhanced safety by eliminating a limit to the prime factor of a parameter.

CONSTITUTION: An arbitrary prime factor is first selected and an enciphering key corresponding to the factor is registered with a public file device 10. Then, a decoding key list corresponding to the factor and the enciphering key is generated and saved in a decoding device 40, together with the factor. Thereafter, an enciphering device 30 receives the public-key of a receiver (decoding device) from the public file device 10, and performs the multiplication of a plain text on an elliptic curve. Then, the device 30 sends the multiplied value as a cryptotext to the decoding device 40. This device 40 calculates an elliptic curve parameter from the cryptotext and selects such a decoding key as corresponding to the parameter, using the decoding key list. Then, the plain text is obtained from the multiplied value of the cryptotext on the elliptical curve, using a remainder theorem.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－282226

(43)公開日　平成６年(1994)10月７日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０９Ｃ　1/00		8837－5L		
Ｈ０４Ｌ　9/06				
9/14				
		8949－5K	Ｈ０４Ｌ　9/ 02	Ｚ

審査請求　未請求　請求項の数１　ＯＬ　（全 12 頁）

(21)出願番号　特願平5－70436

(22)出願日　平成５年(1993)３月29日

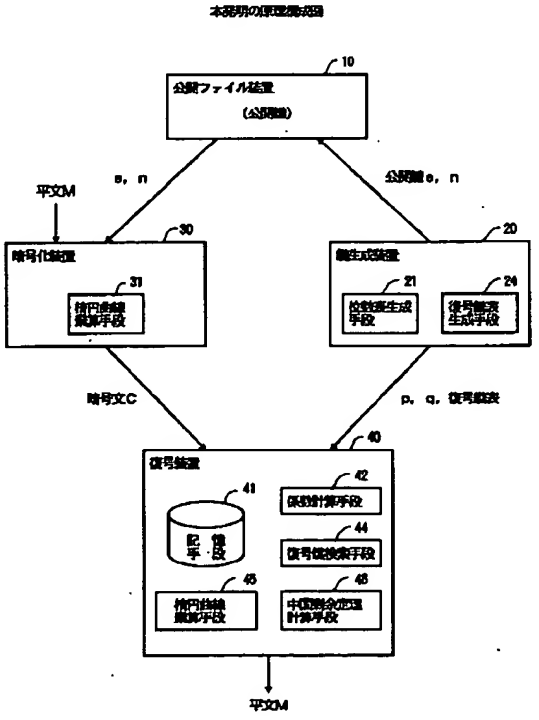
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　桑門　秀典
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　小山　謙二
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　伊東　忠彦

(54)【発明の名称】　楕円曲線に基づく公開鍵暗号方式

(57)【要約】

【目的】　本発明の目的は、パラメータの素数の制限をなくすことにより安全性を一層高めた楕円曲線に基づく公開暗号方式を提供することである。

【構成】　本発明は、任意の素数を選び、素数に対応した暗号化鍵を公開ファイル装置に登録し、素数、暗号鍵に対応する復号鍵表により生成し、素数と共に復号鍵表を復号装置に記憶しておく。暗号化装置は公開ファイル装置より受信者（復号装置）の公開鍵を入手し、平文を楕円曲線上で乗算し、その値を暗号文として復号装置に送信する。復号装置は暗号文から楕円曲線のパラメータを計算し、復号鍵表を用いてパラメータに対応する復号鍵を選び、暗号文をを楕円曲線で乗算した値から中国剰余定理を用いて平文を得る。



1

【特許請求の範囲】

【請求項１】　受信者により５以上の任意の素数を選択し、該素数に対応する公開鍵を登録する公開ファイル装置と、

素数に対して楕円曲線$y^2 \equiv x^3 + ax \pmod n$の位数とパラメータとの関係を示す識別子と該位数の対応を示す位数表を生成する位数表生成手段と、該素数と該位数表生成手段により生成された該位数表から復号鍵を計算し、該復号鍵と該位数表の識別子との対応を示す復号鍵表を生成する復号鍵表生成手段とを含む復号表生成装置とを有する鍵生成装置と、

平文と公開鍵が入力され、該平文を楕円曲線$y^2 \equiv x^3 + ax \pmod n$上で該公開鍵に基づいて乗算する楕円曲線乗算手段を含み、暗号文を出力する暗号化装置と、該素数と復号鍵表を予め記憶しておく記憶手段と、該暗号化装置から取得した該暗号文と該素数から該楕円曲線$y^2 \equiv x^3 + ax \pmod n$のパラメータを計算する係数計算手段と、該記憶手段に記憶されている該復号鍵表より該楕円曲線$y^2 \equiv x^3 + ax \pmod n$のパラメータに対応する復号鍵を検索する復号鍵検索手段と、該暗号化装置から入力された該暗号文を該楕円曲線$y^2 \equiv x^3 + ax \pmod n$上で該復号鍵に基づいて乗算する楕円曲線乗算手段と、該楕円曲線乗算手段により求められた値と該素数から平文を中国剰余定理に基づいて計算し、出力する中国剰余定理計算手段とを含む復号装とを有することを特徴とする楕円曲線に基づく公開鍵暗号方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、楕円曲線に基づく公開鍵暗号方式に係り、特に、ディジタル化された文書を伝送する際の暗号方式における有限のモノイド上の楕円曲線に基づく暗号方式及び暗号方式に用いられる鍵生成装置、暗号化装置及び復号装置における楕円曲線に基づく公開鍵暗号方式に関する。

【０００２】

【従来の技術】１９９０年に楕円曲線に基づく公開鍵暗号（ＫＭＯＶ方式）が提案されている。このＫＭＯＶ方式はパラメータｎ（＝ｐｑ）の素因数分解の困難さに安全性の根拠をおいているものである。ＫＭＯＶ方式は、パラメータの素数ｐ，ｑが$p \equiv q \equiv 2 \pmod 3$または、$p \equiv q \equiv 3 \pmod 4$でなければならないという制限がある。

【０００３】

【発明が解決しようとする課題】しかしながら、従来の公開鍵暗号方式にはＫＭＯＶ方式を用いた方式により暗号方式を用いていたが、法のｎの素因数に制限があるため、この制限内で暗号方式を適用すると鍵の安全性に問題がある。

【０００４】本発明は、上記の点に鑑みなされたもので、パラメータの素数の制限をなくすことにより安全性を一層高めた楕円曲線に基づく公開暗号方式を提供することを目的とする。

2

【０００５】

【課題を解決するための手段】図１は本発明の原理構成図を示す。本発明は、受信者により５以上の任意の素数ｐ，ｑを選択し、素数ｐ，ｑに対応する公開鍵ｅ，ｎを登録する公開ファイル装置１０と、素数ｐ，ｑに対して楕円曲線$E_p\ (0, b) : y^2 \equiv x^3 + b_p \pmod p$，$E_q\ (0, b) : y^2 \equiv x^3 + b_q \pmod q$の位数$b_p$，$b_q$とパラメータｂとの関係を示す識別子と位数の対応を示す位数表を生成する位数表生成手段２１と、素数ｐ，ｑと位数表生成手段２１により生成された位数表から復号鍵を計算し、復号鍵と位数表の識別子との対応を示す復号鍵表を生成する復号鍵表生成手段２４とを含む鍵生成装置２０と、平文Ｍと受信者の公開鍵ｅ，ｎが入力され、平文Ｍを楕円曲線$E_n\ (0, b_M) : y^2 \equiv x^3 + b_M \pmod n$上で公開鍵ｅに基づいて乗算する楕円曲線乗算手段３１を含み、暗号文を出力する暗号化装置３０と、該鍵生成装置２０から受け取った素数ｐ，ｑと復号鍵表を記憶する記憶手段４１と、暗号化装置３０からの暗号文Ｃと素数ｐ，ｑから楕円曲線$E_p\ (0, b_p) : y^2 \equiv x^3 + b_p \pmod p$，$E_q\ (0, b_q) : y^2 \equiv x^3 + b_q \pmod q$のパラメータ$b_p$，$b_q$を計算する係数計算手段４２と、記憶手段４１に記憶されている復号鍵表より楕円曲線のパラメータに対応する復号鍵d_p，d_qを検索する復号鍵検索手段と、暗号化装置３０から入力された暗号文Ｃを楕円曲線$E_p\ (0, b_p)$，$E_q\ (0, b_q)$上で復号鍵d_p，d_qに基づいて乗算する楕円曲線乗算手段４５と、楕円曲線乗算手段４５により求められた値M_p，M_qと、素数ｐ，ｑから平文Ｍを中国剰余定理に基づいて計算し出力する中国剰余定理計算手段４６とを含む復号装置を有する。

【０００６】

【作用】本発明は、５以上の任意の素数ｐ，ｑを選び、ｐ，ｑに対応した暗号化鍵ｅ，ｎを公開ファイル装置１０に登録し、ｐ，ｑ，ｅに対応する復号鍵表を生成し、素数ｐ，ｑと共に復号鍵表を復号装置に記憶しておく。送信者（暗号化装置）は公開ファイル装置１０より受信者（復号装置）の公開鍵ｅ，ｎを入手し、平文$M = (m_x, m_y)$を楕円曲線$E_n\ (0, b_M) : y^2 \equiv x^3 + b_M \pmod n$上でｅ倍した点Ｃを暗号文Ｃとして受信者（復号装置）に送信する。受信者（復号装置）は暗号文Ｃから楕円曲線$E_p\ (0, b_p) : y^2 \equiv x^3 + b_p \pmod p$，$E_q\ (0, b_q) : y^2 \equiv x^3 + b_q \pmod q$のパラメータ$b_p$，$b_q$を計算し、復号鍵表を用いてパラメータ$b_p$，$b_q$を計算し、復号装置側で予め記憶されている復号鍵表を用いてパラメータb_p，b_qに対応する復号鍵d_p，d_qを選び、暗号文Ｃを楕円曲

線でd_p，d_q倍した点M_p，M_qとから中国剰余定理を用いて平文Mを得る。これにより、公開鍵暗号方式として、従来のＫＭＯＶ方式に代わり有限モノイド上の楕円曲線に基づいており、用いる素数に制限がないため、素因数分解がＫＭＯＶ方式よりも難解になり、安全性が高くなる。

【０００７】

【実施例】以下、図面と共に本発明の実施例を説明する。

【０００８】図２は本発明の一実施例のシステム構成を示す。同図のシステムは、公開鍵ｅ，ｎを登録しておく公開ファイル装置１０、公開鍵ｅ，ｎ及び、復号鍵d_p，d_qを生成する鍵生成装置２０、入力された平文Mを公開ファイル装置１０からの公開鍵ｅ，ｎにより平文Mを暗号化し、暗号文Ｃを作成し、出力する暗号化装置３０と、暗号化装置３０から入力された暗号文Ｃを楕円曲線を用いて復号し，平文Mを出力する復号装置４０から構成される。

【０００９】以下、実施例を説明するにあたり、本発明の公開鍵暗号方式における前提条件を説明する。本発明における公開鍵暗号方式は、有限モノイド上の楕円曲線に基づいており、用いる素数に制限のないものである。

【００１０】まず、楕円曲線に関する記号の説明をする。素数ｐとパラメータａ，ｂに対しし、

$y^2 \equiv x^3 + ax + b \pmod{p}$

を満たす点の集合に無限遠点Ｏを加えた集合を楕円曲線E_n（ａ，ｂ）と呼ぶ。本発明の実施例ではパラメータａが零（ａ＝０）の楕円曲線E_n（０，ｂ）を用いる。

【００１１】以下に本発明の一実施例の各装置について説明する。

１．公開ファイル装置

公開ファイル装置１０は、受信者（復号装置）により５以上の任意の素数ｐ，ｑが選択され、この素数に対応した暗号化鍵（公開鍵）ｅ，ｎが登録される。

【００１２】２．鍵生成装置

図３は本発明の一実施例の鍵生成装置の構成を示す。同図に示す復号鍵生成装置２４は、素数生成器２４１、位数表生成装置２４２、２４３及び復号鍵表生成装置２４４から構成される。素数生成器２４１は素数ｐ，ｑを生成し、素数ｐを位数表生成装置２４２に、素数ｑを位数表生成装置２４３に入力する。

【００１３】（１）位数表生成装置

ここで、各位数表生成装置２４２、２４３は、素数生成器２４１から素数ｐ，ｑにより位数表を作成する。位数表生成装置２４２は、素数ｐに対して楕円曲線

E_p（０，ｂ）：$y^2 \equiv x^3 + b \pmod{p}$

の位数とパラメータｂとの関係を示す識別子と位数の対応を示す位数表を生成する。もし、素数ｐが

$p \equiv 2 \pmod{3}$

であれば、位数表生成装置２４２が生成する位数表は、

【００１４】

【表１】

識別子	位数
*	p＋1

【００１５】となる。位数表生成装置２４２は、この位数表を復号鍵表生成装置２４５に出力する。

【００１６】また、位数表生成装置２４３は素数ｑに対して楕円曲線

E_q（０，ｂ）：$y^2 \equiv x^3 + b \pmod{q}$

の位数とパラメータｂとの関係を示す識別子と位数の対応を示す位数表を生成する。もし、素数ｑが、

$q \equiv 2 \pmod{3}$

であれば、位数表生成装置２４３が生成する位数表は、

【００１７】

【表２】

識別子	位数
*	q＋1

【００１８】となり、位数表生成装置２４３はこの位数表を復号鍵生成装置２４５に出力する。

【００１９】ここで、位数表生成装置２４２、２４３は

$p = \pi\pi'$ かつ、$\pi \equiv 2 \pmod{3}$

を満たす二次体Ｚ［ω］上の整数

$\pi = \alpha - \beta\omega$

を求める。この時、位数表生成装置２４２、２４３は以下に示す位数表を生成する。

【００２０】

【表３】

識別子	位数
1	$N_{p0} = p + 1 + (2\alpha + \beta)$
-1	$N_{p1} = p + 1 - (2\alpha + \beta)$
ω^2	$N_{p2} = p + 1 + (\beta - \alpha)$
$-\omega^2$	$N_{p3} = p + 1 - (\beta - \alpha)$
ω	$N_{p4} = p + 1 - (\alpha + 2\beta)$
$-\omega$	$N_{p5} = p + 1 + (\alpha + 2\beta)$

【００２１】位数表生成装置２４２、２４３は、この位数表を復号鍵生成装置２４５に出力し、動作を終了する。

【００２２】（２）復号鍵表生成装置

次に、復号鍵表生成装置２４５は、２つの素数ｐ，ｑと各素数の位数表から公開鍵ｅ，ｎを計算し、復号鍵表を生成し、公開鍵ｅ，ｎ及び復号鍵表を出力する。

【００２３】図４は本発明の一実施例の鍵生成装置の復号鍵表生成装置を説明するための図である。復号鍵表生

5

成装置２４５は、素数ｐ，ｑの入力により使用する復号鍵生成装置１～３を使い分ける。

【００２４】　まず、素数ｐ，ｑが、

$p \equiv q \equiv 2 \pmod 3$

であれば、復号鍵生成装置１に素数ｐ，ｑとそれらの位数表を入力し、復号鍵生成装置１の出力をそのまま、復号鍵生成装置２４５の出力とし、処理を終了する。

【００２５】詳しくは、復号鍵生成装置１は、入力として素数ｐ，ｑと、当該素数ｐ，ｑの位数表が与えられ

識別子	復号鍵
*	d_{p0}

【００２７】とする。但し、これらの表において、左の列の項は識別子を表し、右の列の項はその識別子に対応する復号鍵を表す。これにより復号鍵生成装置１は暗号化鍵ｅ，ｎと復号鍵表を出力する。

【００２８】　次に、素数ｐ，ｑが、

$p \equiv 1 \pmod 3$，$q \equiv 2 \pmod 3$

であれば、復号鍵表生成装置２に素数ｐ，ｑとそれらの位数表を入力し、復号鍵表生成装置２の出力をそのまま復号鍵表生成装置２４５の出力とし、処理を終了する。

【００２９】詳しくは、復号鍵生成装置２は、入力として素数ｐ，ｑと、当該素数ｐ，ｑの位数表が与えられる。ここで、復号鍵生成装置１は、

$gcd(e, N_{p0}) = gcd(e, N_{p0})$

識別子	復号鍵
1	d_{p0}
-1	d_{p1}
ω^2	d_{p2}
$-\omega^2$	d_{p3}
ω	d_{p4}
$-\omega$	d_{p5}

【００３２】とする。但し、これらの表において、左の列の項は識別子を表し、右の列の項はその識別子に対応する復号鍵を表す。これにより復号鍵生成装置２は暗号化鍵ｅ，ｎと復号鍵表を出力する。

【００３３】　さらに、素数ｐ，ｑが

$p \equiv q \equiv 1 \pmod 3$

ならば、復号鍵表生成装置３に素数ｐ，ｑとそれらの位数表を入力し、復号鍵表生成装置２４５の出力とし、処理を終了する。

6

る。ここで、復号鍵生成装置１は、

$gcd(e, p+1) = gcd(e, q+1) = 1$

となる公開鍵ｅをランダムに設定する。そして、以下の式を満たす復号鍵d_{p0}，d_{q0}を計算する。

$e \cdot d_{p0} \equiv 1 \pmod p$，　$e \cdot d_{q0} \equiv 1 \pmod q$．

これにより、復号鍵生成装置１が出力する復号鍵表は、

【００２６】

【表４】

識別子	復号鍵
*	d_{q0}

$= gcd(e, N_{p1})$
$= gcd(e, N_{p2})$
$= gcd(e, N_{p3})$
$= (e, q+1)$
$= 1$

となる公開鍵ｅをランダムに設定する。そして、以下の式を満たす復号鍵d_{pi}（ｉ＝０～３）、d_{q0}を計算する。

【００３０】$e \cdot d_{pi} \equiv 1 \pmod p$（ｉ＝０～３），$e \cdot d_{q0} \equiv 1 \pmod q$．

これにより、復号鍵生成装置２が出力する復号鍵表は、

【００３１】

【表５】

識別子	復号鍵
*	d_{q0}

【００３４】詳しくは、復号鍵生成装置３は、入力として素数ｐ，ｑと、当該素数ｐ，ｑの位数表が与えられる。ここで、復号鍵生成装置１は、

$gcd(e, N_{pi}) = gcd(e, N_{pi})$
$= 1$（ｉ＝０～３）

となる公開鍵ｅをランダムに設定する。そして、以下の式を満たす復号鍵d_{pi}、d_{qi}を計算する。

【００３５】$e \cdot d_{pi} \equiv 1 \pmod p$
$e \cdot d_{qi} \equiv 1 \pmod q$（ｉ＝０～３）．

これにより、復号鍵生成装置３が出力する復号鍵表は、

【００３６】

識別子	復号鍵
1	d_{p0}
-1	d_{p1}
ω^2	d_{p2}
$-\omega^2$	d_{p3}
ω	d_{p4}
$-\omega$	d_{p5}

【００３７】とする。但し、これらの表において、左の列の項は識別子を表し、右の列の項はその識別子に対応する復号鍵を表す。

【００３８】これにより復号鍵生成装置３は暗号化鍵ｅ，ｎと復号鍵表を公開ファイル装置１０または、復号装置４０に出力する。

【００３９】（３）暗号化装置

図５は本発明の一実施例の暗号化装置の構成を示す。暗号化装置３０は楕円曲線E_n（０，b_M）上において入力された平文Ｍに公開鍵ｅ分を乗算する楕円曲線乗算器３１を有する。

【００４０】暗号化装置３０は、入力として、公開鍵ｅ，ｎと平文Ｍ＝（m_x，m_y）が与えられる。但し、$0<m_x, m_y<n$ and gcd（m_x，ｎ）＝gcd（m_y，ｎ）＝１

とする。

【００４１】暗号化装置３０は、楕円曲線E_n（０，b_M）：$y^2 \equiv x^3 + b_M$ (mod n) 上で、

ｅ・m over E_n（０，b_M）

を計算し、その計算結果を暗号文Ｃとする。そして、暗号文Ｃを復号装置４０に出力して処理を終了する。

【００４２】（４）復号装置

図６は本発明の一実施例の復号装置の構成を示す。同図において、復号装置４０は、素数ｐ記憶部４１０、素数ｑ記憶部４１１、第１、第２の係数計算器４２０、４２１、第１、第２の識別子計算器４３０、４３１、復号鍵検索器４４０、４４１、第１、第２の楕円曲線乗算器４５０、４５１、ｐの復号鍵表記憶部４７０、ｑの復号鍵記憶部４７１及び中国剰余定理計算器４６０より構成される。

【００４３】復号装置４０の素数ｐ記憶部４１０は素数ｐを記憶しておき、素数ｑ記憶部４１１は素数ｑを記憶しておく。

【００４４】第１の係数計算器４２０は、暗号化装置３０から入力された暗号文Ｃと素数ｐ記憶部４１０に記憶されている素数ｐから楕円曲線

E_p（０，b_p）：$y^2 \equiv x^3 + b_p$ (mod p)

のパラメータb_pを計算する。

【表６】

識別子	復号鍵
1	d_{q0}
-1	d_{q1}
ω^2	d_{q2}
$-\omega^2$	d_{q3}
ω	d_{q4}
$-\omega$	d_{q5}

【００４５】第２の係数計算器４２１は、暗号化装置３０から入力された暗号文Ｃと素数ｑ記憶部４１１に記憶されている素数ｑから楕円曲線

E_q（０，b_q）：$y^2 \equiv x^3 + b_q$ (mod q)

のパラメータb_qを計算する。

【００４６】第１の識別子計算器４３０は、楕円曲線のパラメータb_pと素数ｐから識別子τ_pを計算する。

【００４７】第２の識別子計算器４３１は、楕円曲線のパラメータb_qと素数ｑから識別子τ_qを計算する。

【００４８】ｐの復号鍵表記憶部４７０は、素数ｐの復号鍵表を記憶し、ｑの復号鍵表記憶部４７１は素数ｑの復号鍵表を記憶する。

【００４９】復号鍵検索器４４０はｐの復号鍵表記憶部４７０からの復号鍵表と第１の識別子計算器４３０から識別子τ_pが入力されると、当該識別子τ_pにより復号鍵表を検索し、復号鍵d_pを取得する。

【００５０】復号鍵検索器４４１は識別子ｑが入力されると、当該識別子τ_qにより復号鍵表を検索し、復号鍵d_qを取得する。

【００５１】第１の楕円曲線乗算部４５０は、暗号化装置３０から入力された暗号文Ｃを楕円曲線E_p（０，b_p）上でd_p倍して、乗算された結果M_pを出力する。

【００５２】第２の楕円曲線乗算部４５１は、暗号化装置３０から入力された暗号文Ｃを楕円曲線E_q（０，b_q）上でd_q倍して、乗算された結果M_qを出力する。

【００５３】中国剰余定理計算器４６０は素数ｐ記憶部４１０からの素数ｐと素数ｑ記憶部４１１からの素数ｑと第１の楕円曲線乗算器４５０、第２の楕円曲線乗算器４５１からM_p，M_qが入力されると、中国剰余定理により、平文Ｍを出力する。

【００５４】詳しくは、復号装置４０は、入力として、暗号化装置３０から暗号文Ｃ＝（c_x，c_y）が与えら

れ、第１及び第２の係数計算器４２０、４２１では、パラメータ

$b_p = c_y^2 - c_x^3 \bmod p$,

$b_q = c_y^2 - c_x^3 \bmod q$

を計算する。

【００５５】第１及び第２の識別子計算器４３０、４３１は、各パラメータb_p、b_qと、各素数記憶部４１０、４１１から得られた素数によりもし、$p \equiv q \equiv 2 \pmod 3$であれば、素数ｐに対する識別子を「＊」、素数ｑに対する識別子を「＊」とする。また、$p \equiv 1 \pmod 3$，$q \equiv 2 \pmod 3$ならば、素数ｐに対する識別子τ_pを、

【００５６】

【数１】

$$\tau_p = \left(\frac{4 b_p}{\pi p} \right) 6$$

の計算結果とし、素数ｑに対する識別子τ_qを、

【００５７】

【数２】

$$\tau_q = \left(\frac{4 b_q}{\pi q} \right) 6$$

【００５８】とし、各々の計算結果を素数ｐに対する識別子τ_p、素数ｑに対する識別子τ_qとする。復号鍵検索器４４０、４４１は、ｐ，ｑの復号鍵表記録部４７０、４７１から復号鍵表を識別子τ_p，τ_qにより検索し、復号鍵d_p，d_qを得る。次に、第１の楕円曲線乗算器４５０、４５１は、楕円曲線

$E_p\ (0, b_p) : y^2 \equiv x^3 + b_p \pmod p$

$E_q\ (0, b_q) : y^2 \equiv x^3 + b_q \pmod q$

上において、

$d_p \cdot C$ over $E_p\ (0, b_p)$,

$d_q \cdot C$ over $E_q\ (0, b_q)$

を計算し、各々の計算結果をM_p，M_qとする。これにより、中国剰余定理計算器４６０は中国剰余定理を用いてM_p，M_qより平文Ｍを計算し、平文Ｍとして出力する。

【００５９】なお、上記実施例の中の説明で用いられている素数ｐ，ｑの桁数は、その積ｎ（＝ｐｑ）の素因数分解の困難さを考慮して決められる。

【００６０】

【発明の効果】上述のように本発明によれば、法ｎの素因数ｐ，ｑに制限がないため、その素因数分解がより難しくり、素数ｐ，ｑの大きさを同じにした場合に、ＫＭＯＶ方式に比べてより安全である。これにより、安全な公開鍵暗号方式を提供することができる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の一実施例のシステム構成図である。

【図３】本発明の一実施例の鍵生成装置の構成図である。

【図４】本発明の一実施例の復号鍵表生成装置を説明するための図である。

【図５】本発明の一実施例の暗号化装置の構成図である。

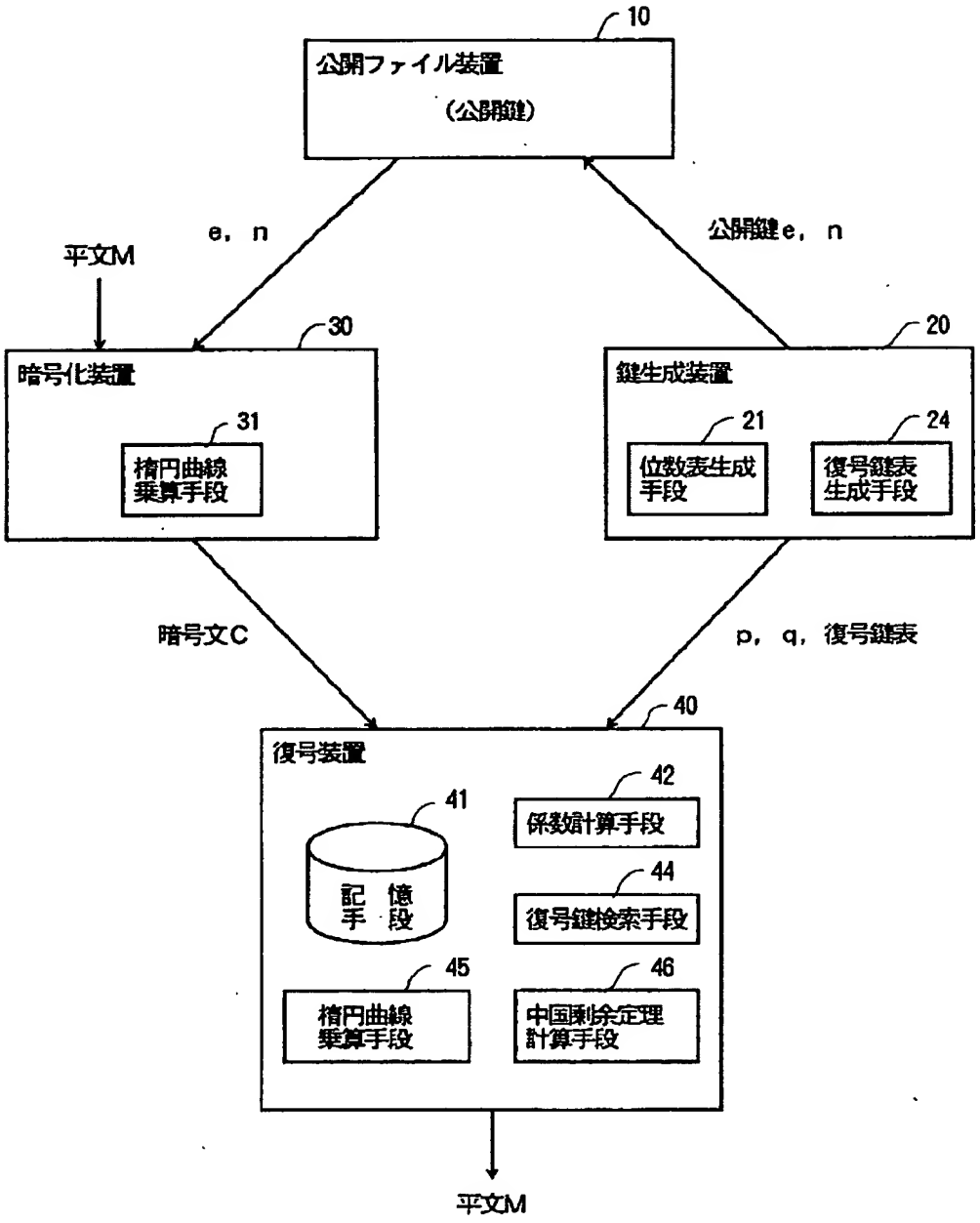
【図６】本発明の一実施例の復号装置の構成図である。

【符号の説明】

１，２，３　復号鍵生成装置
１０　公開ファイル装置
２０　鍵生成装置
２１　位数表生成手段
２４　復号鍵生成手段
３０　暗号化装置
３１，４５　楕円曲線乗算手段
４０　復号装置
４１　記憶手段
４２　係数計算手段
４３　識別子計算手段
４４　復号鍵検索手段
４６　中国剰余定理計算手段
２４１　素数生成器
２４２，２４３　位数表生成装置
２４５　復号鍵表生成装置
４１０　素数ｐ記憶部
４１１　素数ｑ記憶部
４２０　第１の係数計算器
４２１　第２の係数計算器
４３０　第１の識別子計算器
４３１　第２の識別子計算器
４４０，４４１　復号鍵検索器
４５０　第１の楕円曲線乗算器
４５１　第２の楕円曲線乗算器
４６０　中国剰余定理計算器

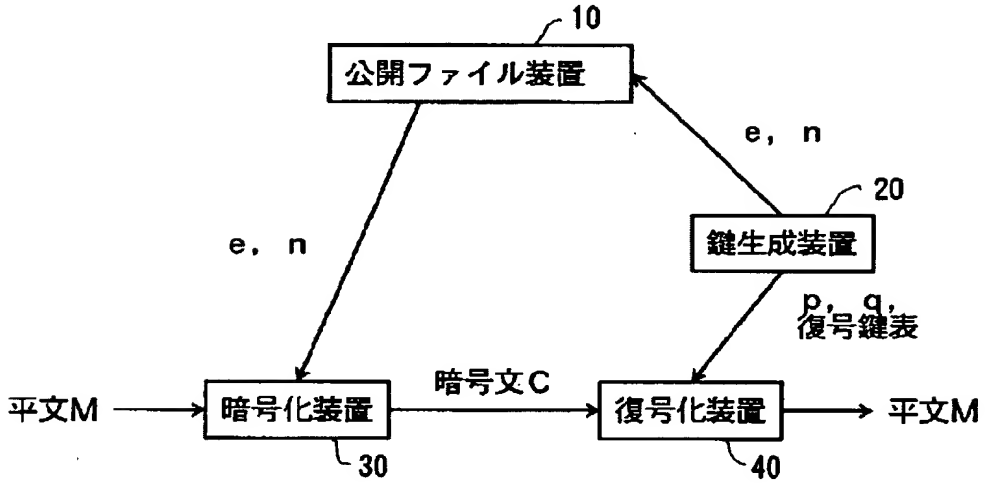
【図１】

本発明の原理構成図



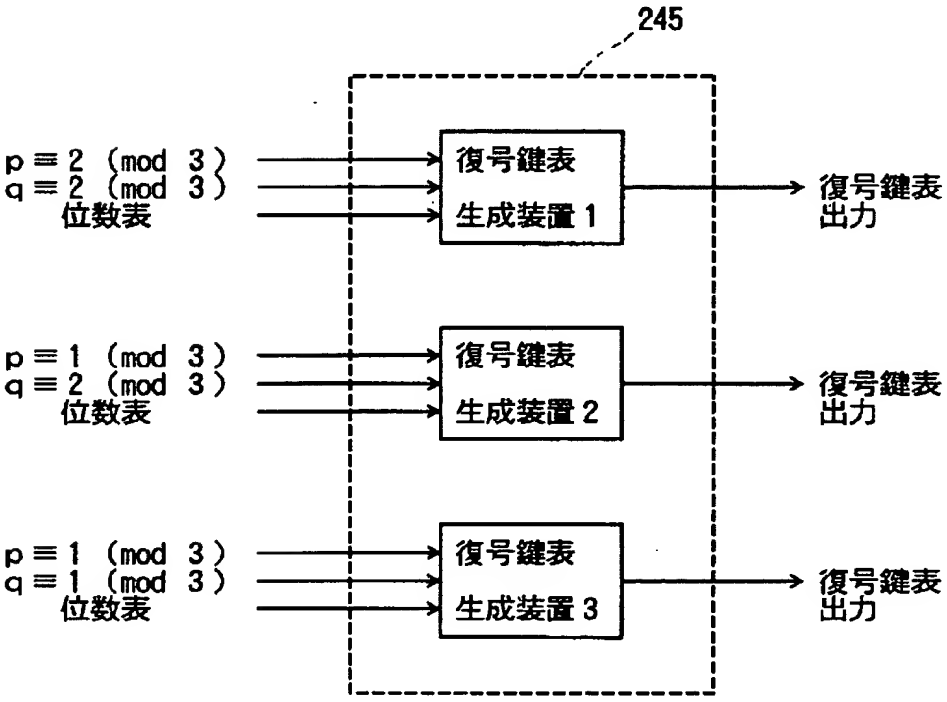
【図２】

本発明の一実施例のシステム構成図



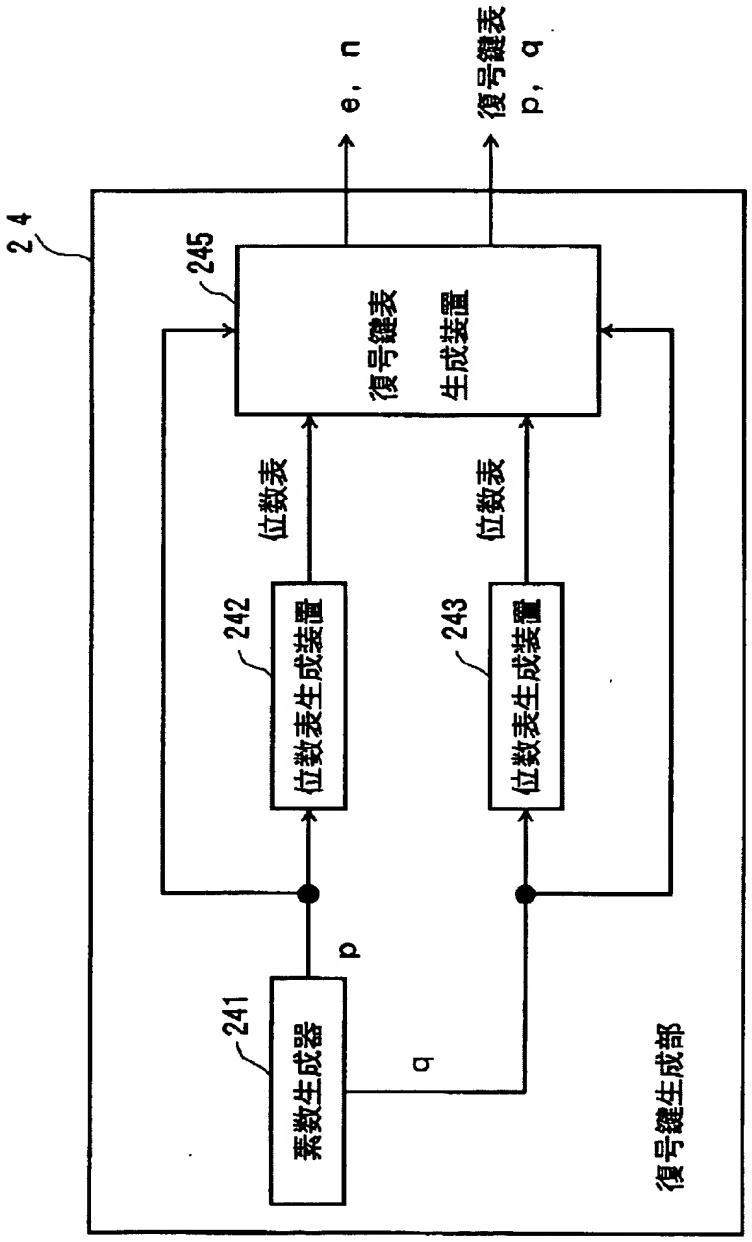
【図４】

本発明の一実施例の復号鍵表生成装置を
説明するための図



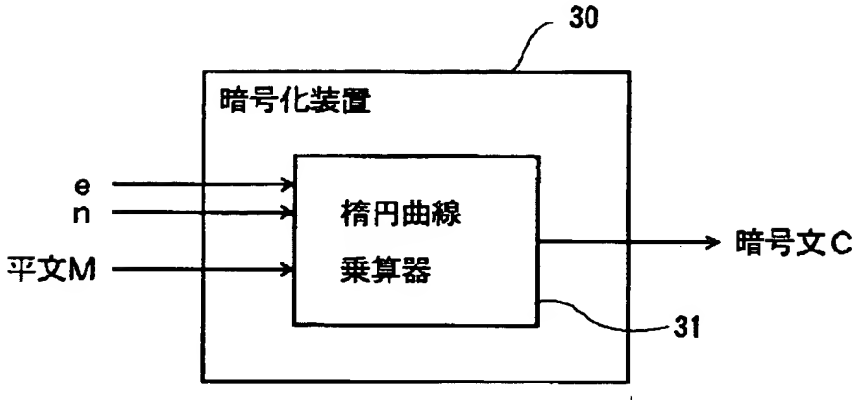
【図３】

本発明の一実施例の鍵生成装置の構成図



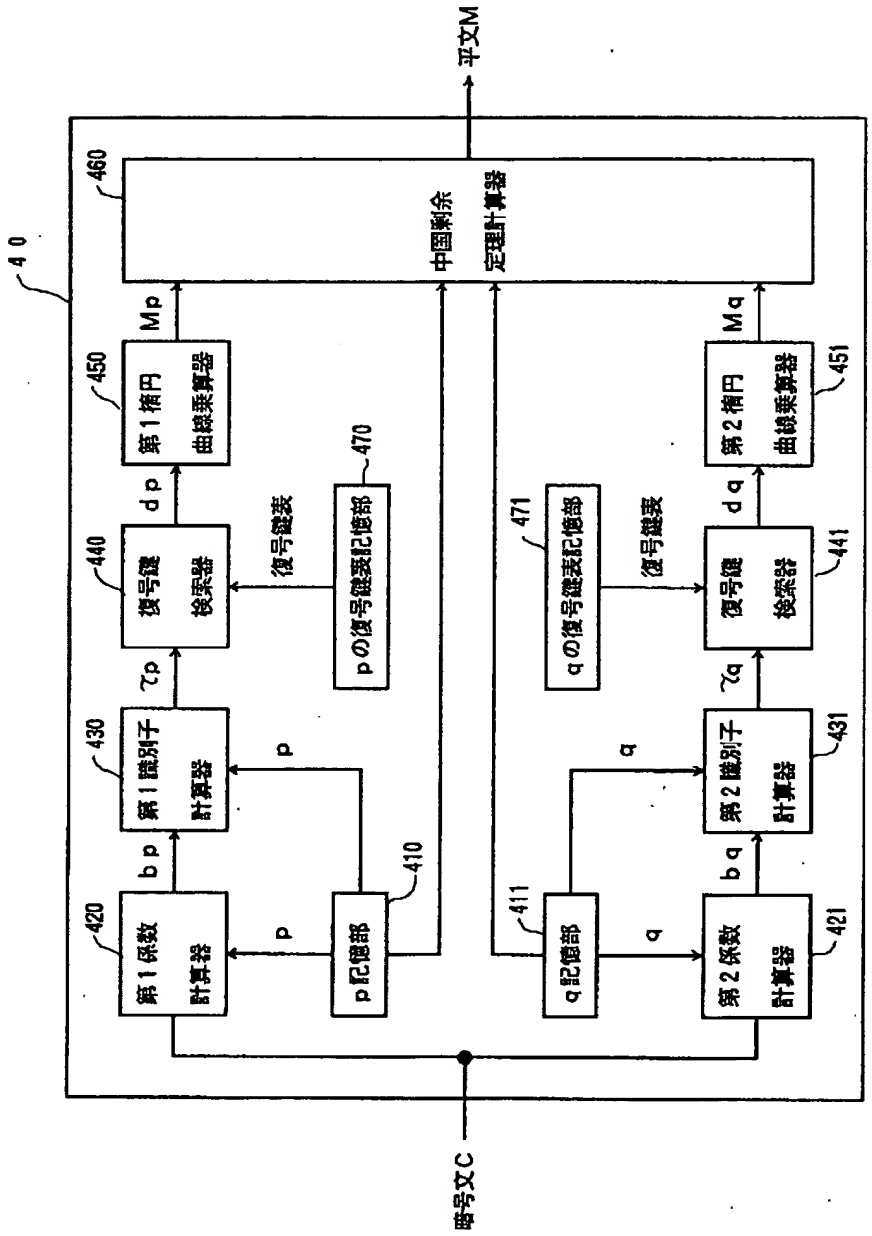
【図５】

本発明の一実施例の暗号化装置の構成図



【図６】

本発明の一実施例の復号装置の構成図



【手続補正書】
【提出日】平成５年５月７日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　受信者により５以上の任意の素数を選択し、該素数に対応する公開鍵を登録する公開ファイル装置と、
素数に対して楕円曲線$y^2 \equiv x^3 + \underline{b}$（mod n）の位数とパラメータとの関係を示す識別子と該位数の対応を示す位数表を生成する位数表生成手段と、該素数と該位数表生成手段により生成された該位数表から復号鍵を計算し、該復号鍵と該位数表の識別子との対応を示す復号鍵表を生成する復号鍵表生成手段とを含む復号表生成装置とを有する鍵生成装置と、
平文と公開鍵が入力され、該平文を楕円曲線$y^2 \equiv x^3 + \underline{b}$（mod n）上で該公開鍵に基づいて乗算する楕円曲線乗算手段を含み、暗号文を出力する暗号化装置と、
該素数と復号鍵表を予め記憶しておく記憶手段と、該暗号化装置から取得した該暗号文と該素数から該楕円曲線$y^2 \equiv x^3 + \underline{b}$（mod n）のパラメータを計算する係数計算手段と、該記憶手段に記憶されている該復号鍵表より該楕円曲線$y^2 \equiv x^3 + \underline{b}$（mod n）のパラメータに対応する復号鍵を検索する復号鍵検索手段と、該暗号化装置から入力された該暗号文を該楕円曲線$y^2 \equiv x^3 + \underline{b}$（modn）上で該復号鍵に基づいて乗算する楕円曲線乗算手段と、該楕円曲線乗算手段により求められた値と該素数から平文を中国剰余定理に基づいて計算し、出力する中国剰余定理計算手段とを含む復号装置とを有することを特徴とする楕円曲線に基づく公開鍵暗号方式。